

## **FINANCIAL AND COMPUTER FRAUD TIPS**

The following information are tips and resources compiled by a fraud investigator with years of experience who also provides resources for further information to help protect you from being a victim of financial and computer fraudulent activities.

- Keep your confidential information private. Your bank or credit card company won't call or e-mail to ask for your account information. They already have it.
- Keep an inventory of everything in your wallet and your PDA, including account numbers. Don't keep your Social Security card in your wallet.
- Stop getting banking and credit card information in the mail. (See "[Go paperless for safer banking.](#)")
- Monitor your bank and credit card transactions for unauthorized use. Crooks with your account numbers usually start small to see if you'll notice.
- If you conduct business online, use your own computer. A public computer is less secure, as is wireless Internet.
- Look for suspicious devices and don't let anyone stand nearby when you use an ATM. Take your card and receipt with you. Keep your PIN in your head, not your wallet.
- Don't store credit card numbers and other financial information on your cell phone. (See "[Is your cell phone spilling your secrets?](#)")

### **PROTECT YOUR COMPUTER FROM VULNERABILITY:**

- Install anti-virus, anti-spyware and firewall protection, and keep them up to date.
- Don't open e-mails from strangers. Malware can be hidden in embedded attachments and graphics files.
- Don't open attachments unless you know who sent them and what they contain. Never open executable attachments. Configure Windows so that the file extensions of known file types are not hidden.
- Don't click on pop-ups. Configure Windows or your Web browser to block them.
- Don't provide your credit card number online unless you are making a purchase from a Web site you trust. Reputable sites will always direct you to a secure page with an URL starting with *https://* whenever you actually make purchases or are asked to provide confidential information.
- Use strong passwords: at least six characters, including at least one symbol and number, and no reference to your name or other personal information. Use a different password for every site that requires one, and change passwords regularly.
- Never send a user name, password or other confidential information via e-mail.
- Consider turning off your computer when you're not using it or at least putting it in standby mode.
- Don't keep passwords, tax returns and other financial information on your hard drive.

## **6 STEPS TO CLEAN UP THE MESS SHOULD YOU BECOME A VICTIM OF IDENTITY THEFT**

1. If you suspect your identity has been compromised, place a fraud alert with the three credit bureaus. When you place an alert, you are entitled to a free copy of your credit report. After that, take advantage of the free annual reports the bureaus are required to give all consumers. Stagger your requests so that you get a report every four months.
  - If you've been phished, contact the bank or company named in the fraudulent e-mail. You also may want to notify the [Internet Crime Complaint Center](#) and forward the e-mail to [spam@uce.gov](mailto:spam@uce.gov).
2. Make an identity-theft report to the police (see Identity Theft Packet under "FORMS" tab on our homepage) and get a copy. File a complaint with the [Federal Trade Commission](#).
3. Close accounts that have been tampered with. Contact each company by phone and again by certified letter (sample letters in our Identity Theft Packet). Make sure the company notifies you in writing that the disputed charges have been erased. Document each conversation and keep all records.
4. Place a seven-year fraud alert or, if you live in a state that allows it, a "freeze" on your credit reports. (See "[Lock your credit away from ID thieves](#).")
5. Begin the process of having the fraudulent information removed from your credit reports. (See "[Don't let credit-report errors fester](#).")
6. Find victim support at the [Identity Theft Resource Center](#).

**[CLICK ON "FRAUD & SCAM DESCRIPTORS" FOR A GLOSSARY OF COMMON TERMINOLOGY](#)**